

SPAM in SOA, and what to do with it

In Summary:

1. Select the message in the inbox
2. Press ctrl-alt-f (shortcut for forwarding an email as an attachment)
3. Send the email to Spam@McAfeeSaaS.com
4. Delete the email from your inbox

Many users will receive unwanted email, and will want to report them or find a way to get less of them. Here's a summary of message types and what to do about them.

All unwanted emails should be forwarded as an attachment to our current anti-spam vendor (McAfee) at **reportspam@alaska.gov**. Additionally, any phishing and other potentially dangerous emails can also be copied (cc'd) to **ExchangeAdmins@alaska.gov**.

The easiest way in Outlook to forward these emails as an attachment is to press **Ctrl+Alt+F**, fill in the recipient(s) and hit Send. There is no need to compose a message to McAfee. Speed is of the most importance.

Phishing e-mails: <http://en.wikipedia.org/wiki/Phishing>

- These are designed to get the recipient to turn over account login credentials such as to bank accounts or email accounts, or to collect personal information (SSN, address, phone #, mother's maiden name) that could eventually be used to compromise such accounts. These emails are typically malformed or modified just enough to initially bypass our McAfeeSaaS filters and the first couple hundred or so of them will reach our users' mailboxes.
- If these are reported within 20 minutes or so of them being sent, there's a chance that McAfee can cut them off quicker than they will on their own.
- If these are reported to ExchangeAdmins@alaska.gov within a few hours of them being sent, there's a good chance that ETS's Messaging team can delete them from other recipients' mailboxes before they get read and potentially responded to, significantly reducing the security risk these have to the State and other State employees.

Scam e-mails (Nigerian scams, also called 419 scams):

http://en.wikipedia.org/wiki/Advance-fee_fraud

- These are designed to get the recipient to start communicating with the scammer via phone or email, in the end to get them to send money, typically by dangling bait that they'll get some large investment in return.
- If these are reported to McAfee it gradually improves their filtering capability to block future scam emails.
- If one of these scam emails appears convincing enough that a state employee is likely to fall for it, please also report it to ExchangeAdmins@alaska.gov and we'll see if we can delete them.

SPAM emails (junk email, unsolicited bulk or commercial email, etc.):

http://en.wikipedia.org/wiki/E-mail_spam

- These are just junk, typically broadcast to thousands or millions of users without much regard to whether the recipient wants to receive them or not. Sometimes people are signed up for periodic newsletter-type emails, depending on the reputation of the sender you can use the Unsubscribe link in it to remove yourself, though the odds are very good that the spammer will then add your name to a list of known-good addresses and while they may not send you the same type of message again, they might sell their list of known-good addresses at a premium price to dozens of other spammers.
 - If these are reported to McAfee it gradually improves their filtering capability to block future spam emails, although we'll never eliminate all of them.
- There is no need to report these to Exchange Admins unless there's some unusual aspect or potentially dangerous security issue with them.